Perfect forms and the Vandiver conjecture

C. SOULÉ

To J.Neukirch

Let p be an odd prime, C the p-Sylow subgroup of the class group of $\mathbb{Q}(\sqrt[p]{1})$, and C^+ the subgroup of C fixed by complex conjugation. The Vandiver conjecture is the statement that $C^+ = 0$. It has been verified when p is less than four million [B-C-E-M].

For any natural integer $i \leq p-2$, let $C^{(i)}$ be the subgroup of C where the Galois group of $\mathbb{Q}(\sqrt[p]{1})$ over $\mathbb{Q}$ acts by the i-th power of the Teichmüller character. Vandiver's conjecture says that $C^{(i)}$ vanishes for all even values of i. Kurihara proved in [K] that $C^{(p-3)} = 0$. His proof uses the existence of a surjective map

$$K_{2n-2}(\mathbb{Z}) \to C^{(p-n)} \underset{\mathbb{Z}}{\otimes} \mathbb{Z}/p$$

and the fact that $K_4(\mathbb{Z})$ is not too big. Here $K_m(\mathbb{Z})$ is the m-th algebraic K-group of the ring of integers, $m > 0$. Since $K_m(\mathbb{Z})$ is finite unless $m-1$ is positive and divisible by four [B], for a fixed value of n there are only finitely many p with $C^{(p-n)} \neq 0$. In this paper we show that, when n is odd and positive,

$$C^{(p-n)} = 0 \quad \text{when} \quad p > v(n)\,,$$

where

$$\log v(n) \leq n^{224n^4}\,.$$

This huge bound follows from a similar assertion about the torsion subgroup of $K_m(\mathbb{Z})$ which in turn comes from a bound on the torsion of the various homology groups of the special linear group $G = SL_N(\mathbb{Z})$ with integral coefficients, $N > 1$. The homology of G coincides, up to finite groups of small cardinality, with the homology of the quotient $Y = X/G$, where X is the symmetric space $SO_N \backslash SL_N(\mathbb{R})$. A finite cell decomposition of a compactification Y^* of Y is provided by the beautiful Voronoi reduction theory [V].

The crucial step in our argument is the fact, that we learnt from O. Gabber, that a bound on the number of cells of a CW-complex as Y^* (and on the number of faces of any given cell in Y^*) provides an explicit upper bound for the cardinality of the torsion subgroup of its integral homology. Such bounds for the Voronoi cell decomposition of Y^* follow from standard

arguments on lattices. Since both steps are exponential in N, we cannot get better than a double exponential estimate for $v(n)$.

In Section 1 we discuss Voronoi's reduction theory. In Section 2 we bound the order of the torsion in the homology of $SL_N(\mathbb{Z})$ (Theorem 1) and in the K-theory of $\mathbb{Z}$ (Theorem 2). In Section 3 we apply these bounds to the Vandiver conjecture (Theorem 4) and to groups related to it by the Iwasawa theory (Theorem 3 and Theorem 5).

It would be interesting to generalize the results above by replacing $\mathbb{Z}$ by the ring of integers in an arbitrary number field.

I thank O. Gabber for telling me about Proposition 3, which was the starting point of this work, as well as J. Buhler, O. Gabber, J. Martinet, J-P. Serre, L. Washington and D. Zagier for helpul comments.

1. Perfect forms

1.1. Let $N \geq 2$ be an integer, let V_N be the vector space of N by N real symmetric matrices, and let $P_N \subset V_N$ be the open cone of all positive definite symmetric matrices. The group $\mathbb{R}_+$ of positive real numbers acts on P_N by multiplication, and the quotient $X_N = P_N/\mathbb{R}_+$ is the symmetric space of $SL_N(\mathbb{R})$.

A matrix A in V_N is said to have *rational nullspace* when the nullspace $\mathrm{Ker}(A)$ of the bilinear form defined by A is spanned by vectors in $\mathbb{Q}^N \subset \mathbb{R}^N$. We let P_N^* be the subset of V_N consisting of all nonzero positive semi-definite symmetric matrices with rational nullspace, $X_N^* = P_N^*/\mathbb{R}_+$ and $\pi : P_N^* \to X_N^*$ the projection map.

The group $GL_N(\mathbb{Z})$ acts upon P_N^* on the right by the formula

$$A \cdot g = g^t\, A\, g\,,\ g \in GL_N(\mathbb{Z})\,,\ A \in P_N^*\,,$$

where g^t is the transpose of g, and P_N is invariant under this action.

Given A in P_N we let $\mu(A)$ be the minimum value of the number $v^t\, A\, v$ where v ranges over all nonzero vectors in the lattice $L = \mathbb{Z}^N \subset \mathbb{R}^N$, and $m(A)$ be the (finite) set of vectors $v \in L - \{0\}$ such that $v^t\, A\, v = \mu(A)$, i.e. the set of minimal vectors.

A form $A \in P_N$ is called *perfect* if $\mu(A) = 1$ and, for any B in P_N such that $\mu(B) = 1$, the equality of sets $m(B) = m(A)$ implies $B = A$.

1.2. It was shown by Voronoi [V] p.110, Thm., that, up to conjugation by $SL_N(\mathbb{Z})$, there are only finitely many perfect forms. To give an upper bound on the number of classes of perfect forms, it is clearly enough to bound the size of their minimal vectors. Let us denote by $\gamma = \gamma(N)$ the *Hermite constant* i.e. the supremum of the quantity $\mu(A)\ \det(A)^{-1/N}$ when A runs over P_N.

We also denote by $s(N)$ the maximum of $\mathrm{card}(m(A))/2$ over all $A \in P_N$ (half the *kissing number* of the corresponding packing of spheres, [C-S] I), where $\mathrm{card}(S)$ denotes the cardinal of a finite set S.

Proposition 1. *Let $A \in P_N$ be such that $\mu(A) = 1$ and $m(A)$ spans the real vector space $\mathbb{R}^N$. Then there exists $g \in SL_N(\mathbb{Z})$ such that any vector $v \in m(A \cdot g)$ has coordinates x_i such that*

$$|x_i| \leq A(N)\,, \quad 1 \leq i \leq N\,, \tag{1}$$

with

$$A(N) = N^{(N-1)}\,\gamma^{N/2}\,. \tag{2}$$

Proof of Proposition 1. (See [M], III 5.2.) Let

$$h(v,w) = \ v^t\,A\,w\,, \quad v, w \in \mathbb{R}^N\,,$$

be the quadratic form defined by A and $h(v) = h(v,v)$. By [Z], Lemma 1.7, since $m(A)$ spans $\mathbb{R}^N$ and $\mu(A) = 1$ we can find a basis of $\mathbb{Z}^N$ made of vectors (e_i) such that

$$h(e_i) \leq N^2\,, \quad 1 \leq i \leq N\,. \tag{3}$$

Up to conjugation by $SL_N(\mathbb{Z})$ and, eventually, the replacement of e_1 by $-e_1$, we may assume that (e_i) is the standard basis of $L = \mathbb{Z}^N$. Let

$$v = \sum_{i=1}^{N} x_i\,e_i$$

be any vector in $\mathbb{R}^N$. For a any integer i, $1 \leq i \leq N$, denote by A_i the matrix of scalar products

$$A_i = (h(v_k, v_\ell))$$

where $v_k = e_k$ when $k \neq i$ and $v_i = v$. Clearly

$$|x_i|^2 = \det(A_i)/\det(A)\,. \tag{4}$$

When v is in $m(A)$, Hadamard's inequality, (3) and the fact that $h(v) = 1$ imply that

$$\det(A_i) \leq N^{2(N-1)}\,. \tag{5}$$

The definition of γ implies

$$\det(A)^{-1} \leq \gamma^N\,. \tag{6}$$

The proposition follows from (4), (5) and (6).

q.e.d.

1.3. Any vector v in $L-\{0\}$ determines a form $\widehat{v} = v\,v^t$ in P_N^*. Given any finite subset $B \subset L-\{0\}$, the *convex hull* of B is the image by π of the subset

$$\left\{ \sum_j \lambda_j\, \widehat{v_j} \,:\, v_j \in B\,,\ \lambda_j \geq 0 \right\}$$

of P_N^*. When A is a perfect form, we let $\sigma(A) \subset X_N^*$ be the convex hull of its set $m(A)$ of minimal vectors.

According to Voronoi [V], §8-15, see also [As], the cells $\sigma(A)$ and their intersections, when A runs over all perfect forms, define a cell decomposition of X_N^*, invariant under $GL_N(\mathbb{Z})$. We equip X_N^* with the corresponding CW-topology. Since there are only finitely many perfect forms modulo the action of $SL_N(\mathbb{Z})$, the quotient space $Y_N^* = X_N^*/SL_N(\mathbb{Z})$ is a finite CW-complex.

Let now

$$B(N) = (2A(N)+1)^N/2\,, \tag{7}$$

where $A(N)$ is defined by (2), and let $k \geq 0$ be an integer.

Proposition 2.

i) *The number of equivalence classes of k-dimensional cells in the Voronoi decomposition of X_N^* is at most*

$$c(k,N) = \begin{pmatrix} B(N) \\ k+1 \end{pmatrix}\,. \tag{8}$$

ii) *Any k-dimensional cell has at most $f(k,N)$ faces, with*

$$f(k,N) = \begin{pmatrix} s(N) \\ k \end{pmatrix}\,. \tag{9}$$

Proof. Let Φ be the set of non zero vectors $v = (x_i)$ in $\mathbb{Z}^N$ satisfying (1). Clearly $\mathrm{card}(\Phi) \leq 2B(N)$. Any cell σ is the convex hull of a subset of $m(A)$, for some perfect form A ([V], §20, [M], VII Thm. 1.12). Therefore, if it has dimension k there exists $g \in SL_N(\mathbb{Z})$ such that the interior of $\tau = \sigma \cdot g$ contains the interior of the convex hull of $(k+1)$ vectors in Φ. There are at most $c(k,N)$ such cells τ.

For the same reason, any face of σ contains the interior of the convex hull of k vectors in $m(A)$. The number of such k-uples of vectors (taken up to sign) is bounded by $f(k,N)$.

q.e.d.

2. Homology of $SL_N(\mathbb{Z})$

2.1. Let $a > 0$, $b > 0$ be integers and

$$\varphi : \mathbb{Z}^a \to \mathbb{Z}^b$$

a $\mathbb{Z}$-linear map. Denote by S the image of φ, by Q the cokernel of φ and by Q_{tors} the torsion subgroup of Q. Denote by $\|\cdot\|$ the standard euclidean norm in $\mathbb{R}^b$ and by (e_i), $1 \leq i \leq a$, the standard basis of $\mathbb{Z}^a$.

Lemma 1. *Let $I \subset \{1, \ldots, a\}$ be a set of indices such that the set of vectors $\varphi(e_i)$, $i \in I$, is a basis of $S \underset{\mathbb{Z}}{\otimes} \mathbb{R}$. Then*

$$\operatorname{card}(Q_{\text{tors}}) \leq \prod_{i \in I} \|\varphi(e_i)\| .$$

Proof. If $E = \mathbb{Z}^b$ we have an exact sequence of finitely generated abelian groups

$$0 \to S \to E \to Q \to 0 . \tag{10}$$

Equip $E \underset{\mathbb{Z}}{\otimes} \mathbb{R} = \mathbb{R}^b$ with the standard scalar product, and both $S \otimes \mathbb{R}$ and $Q \otimes \mathbb{R}$ with the induced scalar product (so that the projection map $E \otimes \mathbb{R} \to Q \otimes \mathbb{R}$ gives an isometry from the orthogonal complement of $S \otimes \mathbb{R}$ onto $Q \otimes \mathbb{R}$). Call $\overline{S}$, $\overline{E}$, $\overline{Q}$ these euclidean lattices. Their arithmetic degrees ([L] V § 2, [S4] VIII 1.4) satisfy the relation

$$\widehat{\deg}(\overline{E}) = \widehat{\deg}(\overline{S}) + \widehat{\deg}(\overline{Q}) . \tag{11}$$

Since $\overline{E}$ is standard we have

$$\widehat{\deg}(\overline{E}) = 0 . \tag{12}$$

Let $P = Q/Q_{\text{tors}}$. Since P is torsion free and spanned by vectors of length at most one, we get

$$\widehat{\deg}(\overline{P}) = -\log \operatorname{covolume}(\overline{P}) \geq 0 .$$

Therefore

$$\widehat{\deg}(\overline{Q}) = \widehat{\deg}(\overline{P}) + \widehat{\deg}(Q_{\text{tors}}) \geq \log \operatorname{card}(Q_{\text{tors}}) . \tag{13}$$

Furthermore, the exterior product $\bigwedge_{i \in I} \varphi(e_i)$ (taken in any order) is a non zero element of the maximal exterior power $\det(S)$ of the lattice S. Therefore, by the Hadamard inequality,

$$\widehat{\deg}(\overline{S}) = \widehat{\deg}(\det(\overline{S})) \geq -\log \| \bigwedge_{i \in I} \varphi(e_i) \| \geq -\sum_{i \in I} \log \|\varphi(e_i)\| . \tag{14}$$

¿From (11), (12), (13) and (14) we conclude that

$$\log \operatorname{card}(Q_{\text{tors}}) \leq \sum_{i \in I} \log \|\varphi(e_i)\| \,.$$

q.e.d.

2.2. Let $(C_\cdot, \partial)$ be a chain complex of free finitely generated $\mathbb{Z}$-modules C_k, $k \geq 0$. Let Σ_k be a basis of C_k and, for any $\sigma \in \Sigma_{k+1}$, let us write

$$\partial(c) = \sum_{c' \in \Sigma_k} n_{\sigma\sigma'}\, \sigma' \,.$$

Define

$$a(k) = \operatorname{Inf}(\operatorname{card}(\Sigma_{k+1}), \operatorname{card}(\Sigma_k)) \tag{15}$$

and

$$b(k) = \operatorname{Sup}\left(\operatorname*{Sup}_{\sigma \in \Sigma_{k+1}} \left(\sum_{\sigma' \in \Sigma_k} n_{\sigma\sigma'}^2 \right)^{1/2}, 1 \right) . \tag{16}$$

Proposition 3. (O. Gabber): *For any $k \geq 0$,*

$$\operatorname{card} H_k(C_\cdot)_{\text{tors}} \leq b(k)^{a(k)} \,.$$

Proof. The homology group

$$H_k(C_\cdot) = \frac{\operatorname{Ker}(\partial)}{\operatorname{Im}(\partial)}$$

is contained in the cokernel Q of the map

$$\partial : C_{k+1} \to C_k \,.$$

For any $\sigma \in \Sigma_{k+1}$, the vector $\partial(\sigma)$ has coordinates $(n_{\sigma\sigma'})$ in the free $\mathbb{Z}$-module $C_k = \mathbb{Z}^{\Sigma_k}$. Therefore

$$\|\partial(\sigma)\| = \left(\sum_{\sigma'} n_{\sigma\sigma'}^2 \right)^{1/2} \leq b(k) \,.$$

The rank t of the image of d is at most $a(k)$. From Lemma 1 we conclude that

$$\operatorname{card} H_k(C_\cdot)_{\text{tors}} \leq \operatorname{card} Q_{\text{tors}} \leq b(k)^t \leq b(k)^{a(k)} \,.$$

q.e.d.

2.3. For any integer $n > 0$ we let $\mathcal{S}_n$ be the Serre class of finite abelian groups which have no element of prime order $p > n$. Given any finite abelian group A, let $B \subset A$ be the maximal subgroup of A lying in $\mathcal{S}_n$ and

$$\mathrm{card}_n(A) = \mathrm{card}(A/B)\,.$$

This quantity depends only on the class of A modulo $\mathcal{S}_n$.

2.4. Let N and k be positive integers, with $k \leq N(N-1)/2$. Let

$$\ell = (N(N+1)/2) - 1 - k\,,$$

and

$$h(k,N) = f(\ell,N)^{c(\ell,N)}\,, \tag{17}$$

where f and c are defined by (8) and (9).

Theorem 1. *The torsion subgroup in the homology of $SL_N(\mathbb{Z})$ is bounded as follows:*

$$\mathrm{card}_{N+1}\, H_k(SL_N(\mathbb{Z}),\mathbb{Z})_{\mathrm{tors}} \leq h(k,N)\,.$$

Proof. We may assume $N \geq 3$ since the homology of $SL_2(\mathbb{Z})$ is well-known (and we do not need it). Let $G = SL_N(\mathbb{Z})$, $X^* = X^*_N$ and $\partial X^* = \partial X^*_N$. Denote by $C.(X^*, \partial X^*)$ the chain complex of the pair of CW-complexes $(X^*, \partial X^*)$ with integral coefficients, by $C.(X^*, \partial X^*)_G$ its coinvariants under the action of G, and by $(C., \partial) = C.(X^*, \partial X^*)_G/(\text{torsion})$ the quotient of this complex by its torsion sub-complex. For all $k \geq 0$, let Σ'_k be a set of representatives, modulo G, of the k-dimensional cells in the Voronoi cell decomposition of X^* which are not contained in ∂X^*. One has

$$C_k(X^*, \partial X^*)_G \sim \bigoplus_{\sigma \in \Sigma'_k} H_0(G_\sigma, \mathbb{Z}_\sigma),$$

where G_σ is the stabilizer of σ and $\mathbb{Z}_\sigma$ its orientation module. Denote by $\Sigma_k \subset \Sigma'_k$ the set of cells σ such that no element in G_σ changes the orientation of σ. When σ lies in Σ_k the group $H_0(G_\sigma, \mathbb{Z}_\sigma)$ is isomorphic to $\mathbb{Z}$, and it is killed by two if σ lies in $\Sigma'_k - \Sigma_k$. Therefore C_k is a free module with basis Σ_k over $\mathbb{Z}$.

Given any $\sigma \in \Sigma_{k+1}$ we have

$$\partial(\sigma) = \sum_{\sigma' \in \Sigma_k} n_{\sigma\sigma'}\, e_{\sigma'},$$

where $|n_{\sigma\sigma'}|$ is at most the number of faces τ of σ in X^* which are equivalent to σ'. Proposition 2 implies that, for any $\sigma \in \Sigma_{k+1}$,

$$\left(\sum_{\sigma' \in \Sigma_k} n^2_{\sigma\sigma'}\right)^{1/2} \leq \sum_{\sigma' \in \Sigma_k} |n_{\sigma\sigma'}| \leq f(k+1,N) \tag{18}$$

and

$$\text{card}(\Sigma_k) \leq c(k,N)\,. \tag{19}$$

¿From (18), (19) and Proposition 3 we conclude that

$$\text{card}\, H_k(C.)_{\text{tors}} \leq f(k+1,N)^{c(k+1,N)}\,. \tag{20}$$

Since $C.$ is torsion free, by the universal coefficient theorem, we have

$$\text{card}\, H^{k+1}(C.,\partial)_{\text{tors}} = \text{card}\, H_k(C.,\partial)_{\text{tors}}\,. \tag{21}$$

On the other hand, given any element g in the group G of order a prime p, the roots of the characteristic polynomial of g are p-th roots of unity, therefore $p \leq N+1$. Furthermore, the stabilizer of any cell of X^* which is not contained in ∂X^* is finite. Therefore the cohomology group $H^k(C.,\partial)$ coincides modulo $\mathcal{S}_{N+1}$ with the equivariant cohomology group $H^k_G(X^*,\partial X^*)$ ([Br], VII.7). From [S5] Proposition 1, we know that

$$H^m(X^*,\partial X^*) = \begin{cases} St^* \text{ if } m = N-1\,, \\ 0 \text{ otherwise,} \end{cases}$$

where St^* is the top cohomology of the Borel-Tits building of SL_N over $\mathbb{Q}$, i.e. the $\mathbb{Z}$-dual of the Steinberg module. Therefore (by the cohomological analog of [Br] VII (7.2))

$$H^k_G(X^*,\partial X^*) = H^{k-N+1}(G,St^*)\,. \tag{22}$$

The long exact sequence of Farrell, [F] Theorem 2 (b), and the Borel-Serre duality [B-S] tell us that

$$H^k(G,St^*) = H_{v-k}(G,\mathbb{Z}) \tag{23}$$

modulo $\mathcal{S}_{N+1}$, where $v = N(N-1)/2$ is the virtual cohomological dimension of G. Indeed, since no element in the group G has order a prime $p > N+1$, the Farrell homology of G lies in $\mathcal{S}_{N+1}$, as follows from the homological analog of the spectral sequence of [Br] X (4.1) (one can also use [Br] X. 3 Exercise 2). In particular, $H_k(G,\mathbb{Z})$ lies in $\mathcal{S}_{N+1}$ when $k > N(N-1)/2$ and the theorem would be trivial in that case. If we combine (20), (21), (22) and (23) we get our assertion.

q.e.d.

2.5. For any $m \geq 1$ let $K_m(\mathbb{Z})$ be the m-th higher algebraic K-group of the integers, and

$$k(m) = h(m,2m+1)\,. \tag{24}$$

Theorem 2. *For any $m > 0$ we have*

$$\mathrm{card}_{2m+2}\, K_m(\mathbb{Z})_{\mathrm{tors}} \leq k(m)\,.$$

Proof. Consider the Hurewicz map of the H-space $BGL(\mathbb{Z})^+$:

$$H : K_m(\mathbb{Z}) \to H_m(GL(\mathbb{Z}), \mathbb{Z})\,.$$

The kernel of H lies in $\mathcal{S}_n$, where n is the integral part of $(m+1)/2$ ([S2] Proposition 3, see also [A] Theorem 1.5). Furthermore

$$H_m(GL(\mathbb{Z}), \mathbb{Z}) = H_m(GL_N(\mathbb{Z}), \mathbb{Z})$$

whenever $N \geq 2m+1$ (cf. for instance [Su], Corollary 8.3). When N is odd, $GL_N(\mathbb{Z})$ is the product of $SL_N(\mathbb{Z})$ by a group of order two, so their homology groups coincide modulo $\mathcal{S}_2$. We now apply Theorem 1 and we get Theorem 2.

q.e.d.

2.6. When $m \leq 5$, $K_m(\mathbb{Z})$ has no p-torsion unless $p \leq 3$ [L-S]. Let us evaluate $k(m)$ when $m \geq 6$.

Lemma 2. *When $m \geq 6$*

$$\log k(m) \leq m^{20m^4}\,.$$

Proof. The following estimates hold:

$$\gamma(N) \leq 1 + \frac{N}{4} \tag{25}$$

([M-H] II (1.5) Remark) and

$$s(N) \leq 2^N - 1 \tag{26}$$

([V] p.107, Lemme) (for sharper estimates, see [K-L] and [C-S] Chapter I, (49) and (50)). When $N = 2m+1$ and $k = m$, we have

$$\ell = \frac{N(N+1)}{2} - m - 1 = (N^2-1)/2\,.$$

By the definitions (17) and (24) we have

$$\log\log k(m) = \log c(\ell, N) + \log\log f(\ell, N)\,. \tag{27}$$

Since

$$c(\ell, N) = \binom{B(N)}{\ell+1} \leq B(N)^{\ell+1}$$

we get

$$\log c(\ell, N) \leq \frac{N^2+1}{2} \log(B(N)) \,. \tag{28}$$

Using (7), (2) and (25) we have

$$B(N) = (2A(N)+1)^N/2 \,,$$
$$A(N) \leq N^{(N-1)} \left(1+\frac{N}{4}\right)^{N/2} \,.$$

Since

$$\log(1+x) \leq \log(x) + \frac{1}{x} \,, \tag{29}$$

we get an upper bound of $\log B(N)$ by a finite linear combination of $\log(N)N^k$ and N^k, $-1 \leq k \leq 4$. Applying (29) again to replace N by m, we get from (26), (9), (27) and (28) a similar upper bound for $\log\log k(m)$, namely

$$\log\log k(m) \leq 12m^4 \log(m) + \varepsilon(m) \tag{30}$$

where

$$\varepsilon(m) = 4\log(2)m^4 + (20\log(m)+14+8\log(2))m^3 + (15\log(m)+22+7\log(2))m^2$$
$$+(5\log(m)+31/2+3\log(2))m + 7\log(m)/2 + 7\log(2)/2 + 5.$$

Since

$$\varepsilon(m) \leq 8m^4 \log(m)$$

as soon as $m \geq 6$, Lemma 2 follows.

q.e.d.

3. Iwasawa theory

3.1. Let p be an odd prime, $k \geq 0$ an integer and $n \in \mathbb{Z}$. Denote by

$$H^k(\mathbb{Z}[1/p], \mathbb{Z}_p(n)) = \varprojlim_{\nu} H^k(\mathrm{Spec}(\mathbb{Z}[1/p]), \mathbb{Z}/p^\nu(n))$$

the étale cohomology groups of the scheme $\mathrm{Spec}(\mathbb{Z}[1/p])$ with coefficients in the n-th Tate twist of the group of p-adic integers. When $n \neq 0$ these groups vanish unless $k = 1$ or 2. It was shown in [S1] and [D-F] that when $m = 2n-k > 1$ and $k = 1$ or 2, there is a surjective map

$$K_m(\mathbb{Z}) \otimes \mathbb{Z}_p \to H^k(\mathbb{Z}[1/p], \mathbb{Z}_p(n)) \,.$$

(In [S1] a Chern class map is defined, the cokernel of which lies in $\mathcal{S}_n$. This is enough for our purpose since Theorem 2 deals only with big primes. In [D-F] a Chern character map is defined, which is always surjective.) Therefore

Theorem 2 gives an upper bound for the torsion of these étale cohomology groups. However, when $k = 1$ one has

$$H^1(\mathbb{Z}[1/p], \mathbb{Z}_p(n))_{\text{tors}} = H^0(\mathbb{Z}[1/p], \mathbb{Q}_p/\mathbb{Z}_p(n)) = H^0(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathbb{Q}_p/\mathbb{Z}_p(n))\,,$$

and this group is zero unless $p \leq n+1$. When $k = 2$ and $n > 0$ is even, the main conjecture, proved by Mazur and Wiles [M-W], tells us that the order of $H^2(\mathbb{Z}[1/p], \mathbb{Z}_p(n))$ is the p-part of the numerator N_n of B_n/n, where the Bernoulli numbers B_n are defined by the identity of formal power series

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}\,.$$

So the interesting case is when $k = 2$ and n is odd, i.e. when m is divisible by 4. The group $K_m(\mathbb{Z})$ is then finite [B] and we get from Theorem 2 the following:

Theorem 3. *Let $n \geq 3$ be an odd integer. Then*

$$\prod_{p \geq 4n-1} \text{card}\, H^2(\mathbb{Z}[1/p], \mathbb{Z}_p(n)) \leq k(2n-2)\,.$$

3.2. Let $\mathbb{Q}(\mu_p)$ be the cyclotomic extension of $\mathbb{Q}$ obtained by adding p-th roots of unity. The Galois group $\Delta = \text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/p)^*$, and we let $\omega : \Delta \to \mathbb{Z}_p^*$ be the Teichmüller character. It is such that

$$g(\zeta) = \zeta^{\omega(g)},$$

for any $g \in \Delta$ and any p-th root of unity ζ. Let C be the p-Sylow subgroup of the class group of $\mathbb{Q}(\mu_p)$. For any $j \in \mathbb{Z}$, denote by $C^{(j)}$ the set of elements $x \in C$ such that

$$g(x) = \omega(g)^j\, x$$

for any $g \in \Delta$. Since Δ has order prime to p, the subgroup C^+ of C fixed by the complex conjugation is the direct sum of those groups $C^{(j)}$ such that j is even and $0 \leq j \leq p-3$. One has [K]

$$C^{(0)} = C^{(p-3)} = 0\,.$$

A short computation ([K], Lemma 1.1) gives that

$$H^2(\mathbb{Z}[1/p], \mathbb{Z}_p(n)) \underset{\mathbb{Z}}{\otimes} \mathbb{Z}/p = C^{(p-n)} \underset{\mathbb{Z}}{\otimes} \mathbb{Z}/p\,.$$

So Theorem 3 implies

Theorem 4. *Let $n > 1$ be an odd integer. If $p > v(n) = k(2n-2)$, one has*

$$C^{(p-n)} = 0\,.$$

From the proof of Lemma 2 one gets

$$\log\log v(n) \leq 192n^4 \log(n) + \varepsilon(n)$$

with

$$\varepsilon(n) \leq 32n^4 \log(n)\,,$$

so that $\log v(n) \leq n^{224n^4}$, if $n \geq 5$.

3.3. Let $L(s, \omega^k)$ be the Dirichlet L-function of the character ω^k, $k \in \mathbb{Z}$. Denote by E the group of units in $\mathbb{Q}(\mu_p)$ and by E/p its quotient by p-th powers.

Theorem 4. *Let $n \geq 5$ be an odd integer, $p > v(n)$, and $m \in \mathbb{Z}$ an integer congruent to n modulo $(p-1)$.*

i) *The group $C^{(n)}$ is isomorphic to $\mathbb{Z}_p/L(0, \omega^{-n})\ \mathbb{Z}_p$.*

ii) *The cyclic group $(E/p)^{(p-n)}$ is spanned by the cyclotomic unit E_{p-n} defined in* [W] *8.3, p. 155.*

iii) *The group $H^2(\mathbb{Z}[1/p], \mathbb{Z}_p(m))$ vanishes and $H^2(\mathbb{Z}[1/p], \mathbb{Z}_p(p-m))$ is a cyclic $\mathbb{Z}_p$-module.*

iv) *When $p > m$ the group $H^1(\mathbb{Z}[1/p], \mathbb{Z}_p(p-m))$ vanishes. When $m > 1$ the group $H^1(\mathbb{Z}[1/p],\ \mathbb{Z}_p(m))$ is a free cyclic $\mathbb{Z}_p$-module spanned by a cyclotomic element.*

Proof. The p-rank of $C^{(n)}$ is less or equal to 1 by Theorem 3 and [W], Theorem 10.9. Its order is known by [M-W]. This proves i).

It is shown in [M-W], 1.10, Theorem 1, that, if $\mathcal{C}$ is the group of cyclotomic units, the abelian group $((E/\mathcal{C}) \otimes \mathbb{Z}_p)^{(p-n)}$ has the same cardinal as $C^{(p-n)}$. Therefore ii) is also a consequence of Theorem 3.

Assertion iii) follows from the equality

$$H^2(\mathbb{Z}[1/p], \mathbb{Z}_p(j)) \otimes \mathbb{Z}/p = C^{(p-j)} \underset{\mathbb{Z}}{\otimes} \mathbb{Z}/p \quad , j \in \mathbb{Z},$$

that we mentionned already.

When $p > m$ the cyclic group $H^2(\mathbb{Z}[1/p], \mathbb{Z}_p(p-m))$ is finite, isomorphic to $\mathbb{Z}_p/N_{p-m}\mathbb{Z}_p$. The exact sequences

$$0 \to H^1(\mathbb{Z}[1/p], \mathbb{Z}_p(j)) \otimes \mathbb{Z}/p \to\ H^1(\mathbb{Z}[1/p], \mathbb{Z}/p(j)) \to\ H^2(\mathbb{Z}[1/p], \mathbb{Z}_p(j))[p] \to 0$$

and

$$0 \to (E/p)^{(p-j)} \to H^1(\mathbb{Z}[1/p], \mathbb{Z}/p(j)) \to C[p]^{(p-j)} \to 0\,,$$

valid when $j \not\equiv 1$ modulo $(p-1)$, and the previous discussion on H^2 prove that $H^1(\mathbb{Z}[1/p], \mathbb{Z}_p(m))$ is always cyclic over $\mathbb{Z}_p$ and that, if $p > m$, the group $H^1(\mathbb{Z}[1/p], \mathbb{Z}_p(p-m))$ vanishes. When $m > 1$, $H^1(\mathbb{Z}[1/p], \mathbb{Z}_p(m))$ is spanned

by a cyclotomic element since the index of cyclotomic elements [S3] is the cardinality of $H^2(\mathbb{Z}[1/p], \mathbb{Z}_p(m))$ ([B-K], (6.8) and (6.9)).

q.e.d.

3.4. By the argument of [W], Theorem 8.14, together with [M-W], 1.10 Theorem 1, $C^{(p-n)}$ is different from zero if and only if the cyclotomic unit E_{p-n} of [W], 8.3, is a p-th power. Let us assume that this happens with probability $1/p$ (compare [W] loc.cit., Remark), and fix an odd integer n. The probability that there exists a prime $p \leq x$, with $p \geq 37$ (the first irregular prime), such that $C^{(p-n)} \neq 0$ is thus bounded above by

$$\sum_{37 \leq p \leq x} \frac{1}{p} \sim \log\log(x) - 2.56\,.$$

When $x = 4.10^6$ [B-C-E-M] the right hand side is 0.16, and when $x = v(5)$ a good estimate for $\log\log(x)$ is 14.10^4. In other words, Theorem 3 leaves far enough room for Vandiver's conjecture to be wrong!

References

[A] D. Arlettaz: The Hurewicz homomorphism in algebraic K-theory, *J.P.A.A.* **71** (1991), 1-12.

[As] Ash, A.: Polyhedral reduction theory in self-adjoint cones, in *Smooth Compactification of Locally Symmetric Varieties, Lie Group s: History, Frontiers, and Applications, vol. IV*, by Ash, A., Mumford, D., Rapoport, M. and Tai, Y., Math. Sci. Press, Brookline, Mass., 1975.

[B-K] S. Bloch and K. Kato: L-functions and Tamagawa numbers of motives. *In* The Grothendieck Festschrift, vol. 1, *Progr. Math.* **86** (1990), Birkhäuser, Boston, 333-400.

[B] A. Borel: Stable real cohomology of arithmetic groups, *Ann. Scient. Ec. Norm. Sup.* 4ème série, t. 7 (1974), 235-272.

[B-S] A. Borel and J-P. Serre: Corners and arithmetic groups, *Comment. Math. Helv.* **48** (1974), 244-297.

[Br] K.S. Brown: Cohomology of groups, *Graduate Text in Math.* **87**, Springer-Verlag.

[B-C-E-M] J. Buhler, R. Crandall, R. Ernvall and T. Metsänkylä: Irregular primes and cyclotomic invariants up to four million, *Math. Comp.* **61** (1993), 151-153.

[C-S] J.H. Conway and N.J.A. Sloane: Sphere Packings, Lattices and Groups, *Grundlehren* **290**, Springer-Verlag.

[D-F] W. Dwyer and E. Friedlander: Algebraic and etale K-theory, *Trans. Amer. Math. Soc.* **272** (1985), 247-280.

[F] F.T. Farrell: An extension of Tate cohomology to a class of infinite groups, *J.Pure and Applied Alg.* **10** (1977), 153-161.

[K-L] G.A. Kabatiansky, V.I. Levenshtein: Bounds for packings on a sphere and in space, *Problems of Information Transmission* **14** (1978), 1-17.

[K] M. Kurihara: Some remarks conjectures about cyclotomic fields and K-groups of $\mathbb{Z}$, *Compositio Math.* **81** (1992), 223-236.

[L] S. Lang: Introduction to Arakelov theory, (1988), Springer-Verlag.

[L-S] R. Lee and R.H. Szczarba: On the torsion in $K_4(\mathbb{Z})$ and $K_5(\mathbb{Z})$, *Duke Math. Journal* **45** No. 1 (1978), 101-130, with an Addendum by C. Soulé, 131-132.

[M] J. Martinet: Les réseaux parfaits des espaces euclidiens, (1996), Masson.

[M-W] B. Mazur and A. Wiles: Class fields of abelian extensions of $\mathbb{Q}$, *Invent. Math.* **76** (1984), 179-330.

[M-H] J. Milnor and D. Husemoller: Symmetric bilinear forms, *Ergebnisse* **73** (1973), Springer-Verlag.

[S1] C. Soulé: K-Théorie des anneaux d'entiers de corps de nombres et cohomologie étale, *Invent. Math.* **55** (1979), 251-295.

[S2] C. Soulé: Opérations en K-théorie algébrique, *Canad. Journal of Math.* **37**, (1985), 488-550.

[S3] C. Soulé: Eléments cyclotomiques en K-théorie, *Astérisque* **147-148**, (1987), 225-257.

[S4] C. Soulé, D.Abramovich, J.-F.Burnol and J.Kramer: *Lectures on Arakelov geometry*, Cambridge Studies in Advanced Mathematics **33**, (1992), Cambridge University Press.

[S5] C. Soulé: On the 3-torsion in $K_4(\mathbb{Z})$, *Topology*, to appear.

[Su] A.A. Suslin: Stability in algebraic K-theory, *Lecture Notes in Math.* No. 966 (1982), 344-356.

[V] G. Voronoi: Nouvelles applications des paramètres continus à la théorie des formes quadratiques I, *Crelle* **133** (1907), 97-178.

[W] L.C. Washington: Introduction to cyclotomic fields, 2^{nd} edition, *Graduate Text in Maths.* **83** (1996), Springer-Verlag.

[Z] S. Zhang: Positive line bundles on arithmetic surfaces, *Annals of Math.* **136** (1992), 569-587.

C.N.R.S. and I.H.E.S., 35 Route de Chartres, 91440, Bures-sur-Yvette, France.